Fight Against Phishing Attacks Among Internet Banking User: A Knowledge Management Technique

Fadare Olusolade Aribake and Zahurin Mat Aji
Universiti Utara Malaysia {fadareolusolade@gmail.com, zahurin@uum.edu.my}

ABSTRACT

Global growth in the usage of internet has led to the expansion of Internet Banking. Acceptance of IB among banking users has improved due to the suitability offered. However, a few associated Internet networking risks have increased the possibility of encountering phishing attacks. Phishing attack refers to the most defiant security threats that are often perpetuated by conning user's information, whereby personal information is inadvertently disclosed, sensitive information is deleted, and other related resources are destroyed. To handle the challenge of phishing attacks, knowledge management can be used as a strategy in improving existing products and services, especially in producing essential innovations that may secure the role of banks. Such technological innovations lead to the strengthening of Knowledge Management (KM) in improving performance with the linking of individuals, procedures, and knowledge. To become more efficacious in the era of the knowledge age, organizations need to understand and implement various strategic management techniques. Hence, the paper tries to clarify the role of KM in strengthening its usage in the area of internet banking in fighting against phishing attacks. Once users become more familiar with technology, they tend to have higher anticipations towards technology.

Keywords: Internet Banking, Phishing Attacks, Knowledge Management.

I INTRODUCTION

Technology has been seen to be the basic and significant part of financial success. In the last 20 years, the development of technology in business has impacted individuals in a way due to its various benefits (Khedmatgozar & Shahnazi, 2018). Development of technology has several inferences unto the banking sector. Reputation of the banking sector in today's financial growth and expansion cannot be undermined globally. Today the use of internet proposes to banking sector varied range of applications technologies like internet banking which are used in keeping up with the users, in reducing transaction costs, and quicken banking transactions. Besides, the acceptance and approachability of the internet have been a significant factor as it delivers the support for internet banking services to take place (Usman, 2018). Thus, banks worldwide have moved speedily to the era of technological changes whereby customers are exposed to internet banking platforms (Mann, 2017; Chauhan & Choudhary, 2016). Nevertheless, as people are more starting to regularly depend on such online transactions especially during the Covid-19 pandemic, numerous scams, and swindling activities are mushrooming including phishing attacks (Stafford, 2020; Aboobucker & Bao, 2018).

Even though internet banking has extensively been adopted in many advanced countries, users in the developing countries are slower than anticipated (Akgül, 2018; Kamwibua, 2017; Aribake, 2015) because of a low level of trust in the online transaction platform especially on the insecurity or lack of confidence (Viswanadham, 2017; Kaabachi, Ben Mrad, & Petrescu, 2017). Though all transactions requires some degree of trust, those that are approved within the uncertain and impersonal conditions of the internet need considerable points of trust due to the high level of risk generally allied with online transactions (Viswanadham, 2017; Gao & Waechter, 2017). Thus, banking institutions must pay proper consideration in defending their user's information from unlawful individuals who might be requesting various confidential details for deceitful purposes.

Such technological innovations lead to the strengthening of Knowledge Management (KM) in improving performance via the connection of individuals, procedures, and knowledge. This is viewed as appropriate since knowledge has been recognized as a valuable commodity that is embedded in products especially high-technology products and services (Apak, Tuncer, Atay & Koşan, 2012). To be successful in today's challenging organizational environment, companies need to learn from their past errors and not reinvent the wheel again and again. This paper is organized to explain the role of KM in strengthening its usage in the area of internet banking in fighting against phishing attacks.

II LITERATURE REVIEW

A. Phishing Attack

Phishing has been a web security threat that has fascinated the consideration of both academicians and company researchers that can be regulated by firewalls or any form of encryption software (Jain & Gupta, 2017). Thakur and Kaur, (2016) emphasized that phishing was first mentioned on the Internet via a set of hackers in the year 1996, who stole America Online (AOL) accounts by deceiving ignorant AOL users into unveiling their passwords (Carella, Kotsoev, & Truta, 2017). Phishing has severely grown-fully becoming a real threat to security globally and a money-spinning criminal business model (Gupta, Agrawal, & Yamaguchi, 2016). Based on the report by the international anti-phishing working group , released in the year 2016, that year was considered as the worst year in history for phishing scams having 1,220,523 as total figure of attacks indicating a 65% upsurge over the number recorded in the year 2015 (Pymnts, 2017).

Phishing attack has been seen to be a critical risk in an online domain, being a crime whereby a perpetrator sends some designed fake websites that appear to come from a trusted brand or organization in a way of targeting or tricking online users to disclose sensitive info and to gain entrée to their details, such as an address, credit card, username and phone number (Jain, & Gupta, 2016). Federal law enforcement associates of United State have acknowledged phishing attack as a crime involving several individuals that form a professional criminal network such as money laundering (Baykara, & Güre, 2018; Nero, Wardman, Copes & Warner, 2011). Phishing has become a relatively simple way of exploiting not only the average internet banking users but also the institutions that offer the services (Dixit, 2016; Mann, 2017). Therefore, banking institutions need to always install security modules such as anti-virus and keyboard protection on user's devices.

B. Knowledge Management

The purpose of KM is to accomplish knowledge more efficiently and competently. Knowledge advances individual's capacity in meeting their needs and extends the diversity of choices open to them in all areas of their lives. Besides, KM can be the next source of competitive advantage as it has become a mainstream priority for companies of all sizes (Ragsdell, 2009). Similarly, the rapid advancement of internet infrastructure has increased the efficiency of KM. Both knowledge sharing as well as re-use need to be encouraged and recognized at the individual user's level as well as the banking level. KM must be an eye-opener to attain planned business objectives. For instance, the failure of imposing new technical infrastructures that are either unsuitable to respective work environments, or where users are not willing to share knowledge is an ample indication in strengthening KM in organizations (Mills & Smith, 2011). Nevertheless, establishments are gaining skills and competence in managing inner knowledge and smearing it on the attainment of the organizational goals and observing in the direction for fresh bases of knowledge that are not essentially found within the restrictions of the establishment (Rashed, 2016). Hence, there is a need for having KM creativity to become a solution for such problems, which brings together users, processes, and technology that can support organizations to accomplish their goals and visions.

Administrative knowledge is not envisioned in replacing specific knowledge but to match it via making it stronger, more coherent, and more broadly applicable. Moreover, the success of any organization gradually depends on its capacity to analyse, allocate, sustain, yield, and gather knowledge. KM was primarily defined as the procedure of smearing a systematic method to the seizure, structure, management, and distribution of knowledge throughout an organization to work faster, reprocess best practices, and reduce costly rework from project to project (Nonaka and Takeuchi, 1995). KM signifies a thoughtful and systematic approach to guarantee the full operation of the organization's knowledge base, coupled with the potential of individual knowledge base skills, competencies, thoughts, innovations, and ideas to create a more efficient and effective organization. Through the practices of KM, an organization focuses on the systematic exploitation and reuse of knowledge by identifying the administration's modest position in defining tactical gaps in its prevailing knowledge and to gain more on individual knowledge (Bloodgood, 2019).

C. Role of Knowledge Management in Strengthening Internet Banking

The banking system of today has been deep in greater risk ascending from a universal economy letdown. The banking sector, the ultimate drivers of modernization, is fighting to emerge from both financial letdown and misery by apprehending and retentive more reliable and steady users in the monetary phase (Olodude & Oladejo, 2013). The presence of internet banking has enabled the banking sector to handle a huge volume of data and manage various banking transaction processes. However, at the same time, internet banking has also caused various challenges and setbacks. Therefore, the usage of information technology towards managing knowledge must grant KM a new dimension. Living

in a society where access to technology is becoming more significant, skills possessed by internet banking users can enable them to enhance their sense of self-worth, confidence, and security. Eventually, knowledge-intensive organizations have to gradually initiate KM in strengthening internet banking by advancing their tactics and broaden performance (Sukumaran, et al., 2018;. These benefits are substantially connected to diverse reassurances in performance such as improvement in the area of choice making, enlightening the user relationship administration, generate new value via means of new facilities innovations, and producing supplementary dealings (Sukumaran, et al., 2018) for internet banking users.

Distribution of incomparable products and services to internet banking users can strengthen user's satisfaction and volume of sales, while banking sectors will notice the influence of knowledge advancement over their performance (Cebi, Aydin, & Gozlu, 2010; Bogner & Bansal 2007). Implementation of KM has offered diverse unified supports to the IB platform, rendering it to make use of its funds proficiently and successfully (Cebi, et al., 2010). Effective implementation of KM application offers unified and multilayered assistances such as performing activities of knowledge, performance procedure, the performance of employees, performance on market and performance on the organization as a whole which affect each other in one way or the other via direct and indirect in the banking sectors (Sukumaran, et al., 2018; Memon, Rizvi & Syed, 2017). However, most of the available internet banking platforms still facing numerous issues comprising of large-scale competition for users' deposits, withdrawal, insecurity, loans, growing users demands, shaking income restrictions, and the essential in keeping up with the new monetary technologies in abetting IB transactions and services (Rashed, 2016; Olodude, et al., 2013). Hence, the broader the opportunity on the internet banking platform is, the stronger the capability of users towards their KM while on the platform.

Transferring of KM ideas in the aspect of the banking sector has been fast compared to other related fields (Omotayo, 2015; Apak, et al., 2012). Recently, KM has been used as an actual avenue to address the apprehending and transmission of knowledge (Memon, et al., 2017; Uğurlu & Kızıldağ, 2013). The study of Hislop, Murray, Shrestha, and Syed (2018) emphasized KM as watchful and orderly organization of knowledge done via allocating, producing, and smearing to enhance value by recycle, which is skilled via nourishing the appreciated lessons learned (Meihami and Meihami, 2014). Besides, KM intends to endure a lasting modest benefit through keeping organizational knowledge and enhance the eminence, worth, mindfulness, and transferability of info safety knowledge among security personnel across organizations (Lee, Choi & Lee, 2020; Jennex & Durcikova, 2019). With regards to internet banking, knowledge is required in the selection of suitable choices concerning choosing appropriate information controls, strategies, and measures in a way of put on proper measures that can central on enhanced performance while on the system (Eslamkhah & Hosseini Seno, 2019).

III KNOWLEDGE MANAGEMENT AS A TECHNIQUE TO FIGHT AGAINST PHISHING ATTACKS

Phishing has been recognized as one of the terminal attacks (Chin, Xiong, & Hu, 2018). Banking institutions throughout the world have spent a fortune on modern tools and technology to protect internet banking users from being the victim of any basic social engineering harm. Being too dependent on technology in safeguarding their network, the institutions tend to ignore on the human aspects (Robb, 2020). For instance, they disregard the importance of knowledge sharing that need to be regularly communicated to their employees and individual customers. Organizations and customers should communally work hand in hand in a way of merging their existing knowledge in generating a new one (Olodude, et al., 2013). For KM to be effectively shaped and applied in any organization, serious elements such as related policy ought to be linked to organizational objective in attaining benefits. In addition, both employees and customers should be given opportunities to contribute valuable and constructive ideas towards the betterment of the institutions (Omotayo, 2015; Merlyn & Välikangas, 1998).

Educational training is vital on KM to enable internet banking users to fight against phishing attacks. Educational training equips users with the necessary skills to identify a phishing scam. Online phishing communities accumulate data repositories that allow users to share useful information about phishing incidents, creating a knowledge base for online users (Perry, 2020; Baadel, Thabtah, & Majeed, 2018). Besides, phishing attacks get more sophisticated daily with attackers engaging in diverse strategies. Thwarting these attacks is possible through active communication towards strengthening KM by bringing both safety and secured messages on the platform (Jensen, Durcikova & Wright 2017; Jang-Jaccard & Nepal, 2014). These messages must not just caution users towards the widespread deceitful transactions but also to reassure them. KM is one of the most well-known theoretical tactics for the study

of online communication that helps in enabling messages on phishing prevention (Jensen, et al., 2017).

Cassim (2014) and Larson (2010), emphasized that legislation needs to be put in place to grant large-scale damage towards any phishers against internet services providers in hopes that will inspire them in playing their role in the fight against phishing attacks. Individual users of internet banking will always be curious in clicking on links while on the platform, since most of the users do not always pay vigilant attention when on the internet banking platform (Palmer, 2020). As phishers constantly review their tactics, human elements remain the weakest link. Oftentimes phishing emails look so real in tricking users into falling victim (Stafford, 2020). Capitalizing on educational training to keep users on their toes is a smart means of reducing the risk of any invasions (Palmer, 2020). Educational training can be sent to internet banking users by email with links. Monitoring how individuals partake by making them aware that imitation phishing experiments need to be carried out which are measured on their aptitudes to appropriately recognize phishing emails (Hong, 2012). Therefore, there is a need for global educational training that phishing is the root cause of most cyberattacks. Now all needed is to create a general understanding for individuals on how to be more educated and trained in straightening users gaining more on KM to thwart phishing attacks. This does not work as a one-time training; it must be multi-faceted to fully minimize the threat and happen oftentimes for the message to stay fresh with the users.

Once having the proper education, one should fight against any phishing attack through individual practices (Stafford, 2020; Daniels, & Oberly, 2019; Hong, 2012). This implies conceptualization of work exactly the way they are carried out. Individual practices require to be established for effective enhancement, and user's security (Lord, 2020). In addition, such practice facilitates the individual improvement without being the source of error. The individual improvement and enhancement can be achieved through continuous learning. Practice is a proper procedure to enrich and nurture one's creativity in handling respective tasks (Schon, 2015). Educational training and individual practices are vital to fight against phishing attacks. Besides, the notion of practice indicates recurrent activities in line with certain principles and ideologies in a way of attaining the precise goal (Siriwardena & Gillam, 2014). Regular and frequent training is required to ensure effectiveness for users in protecting them from malicious attacks (Palmer, 2020). Multi factors verification help in offering a strong barrier against phishing attacks since it entails an extra step for hackers to overcome in conducting successful attack. The individual practice approach anticipates that one can only understand knowledge concerning the context in which it was generated. Therefore, quality advancement techniques can be used in improving individual practice which can always strengthen individual relationships and loyalty.

IV DISCUSSION

KM in banking is no different from other industries but the growing complexity of financial activities makes the implementation of its applications more challenging. Banks have realized the key role of KM in advancing an edge in the competitive field of managing risks, reducing fraud and ensuring compliance (Chigada, 2014). Study from Frauenstein, (2013) pointed out that banks should be tactically aligned with internet banking users to be aware on the occurrence of phishing attacks occur in order to offer better services. This is vital since some of the factors that contribute to the success of phishing attacks are weak organizational policies, negligence in human behaviour and inadequate technology controls. Therefore, both banks and their customers ought to be educate and trained on the importance of those factors mitigating security threats.

Internet banking customers can be trained on security awareness' by having a rapid and easy access to a complete library read-to-use content and material. This can be achieved through various forms such as adding the content to a bank's website, email newsletters, statement stuffers, or placing posters inside the banking halls of various branches (Sundaram, Thomas, & Agilandeeswari, 2019). However, training users on the issue of phishing attacks can be challenging and requires a determined effort by all bank stakeholders. Once users are aware and educated on phishing scams, they will be more cautious and less likely to fall into such suspicious agenda. As for the policymakers, best practices are required to be devised and strictly followed. Moreover, the banking sectors needs to collaborate with the internet banking providers to come up with phishing proof mechanisms to guarantee the integrity of transactions while improving users' levels of trusts (Bhasin, 2016).

To successfully instill awareness among the internet banking users, the banking industry must recognize KM as one of the top priorities in coming up with relevant and effective strategy to cope with related challenges. The integration of KM into internet banking actions facilitates in the provision of more accurate understanding of KM as an enabler of information strategy specifically for the internet banking platform.

V CONCLUSION AND FUTURE RESEARCH

Security is seen to be a fundamental issue regarding the banking industry. Despite the growing penetration of internet banking by its users, several issues have aroused that gave doubt towards internet security due to phishing attacks. Fight against phishing attacks has considerable potential to enhance customer bank relationships and likewise add value to the bank by retaining and gaining new customers. KM technique request is supposed to be the desires of the banking sectors in relations of offering knowledge-oriented support in giving and strengthening learning opportunities to internet banking users. However, concern for internet banking users is for banks to guarantee that transactions on the internet banking platform are protected from phishing attacks.

To be effective, educational training and individual practices need to be implemented and use continuously. Likewise, improvement is deemed necessary on the part of banking institutions as well as their customers' participation in solving problems by imparting related knowledge and widening their experience in a way of accomplishing strategic aims in the long run. Once become more familiar with educational training and individual practices, users tend to have higher confidence while using the online platform. Hence, KM can be used as a technique to strengthen the internet banking user in fighting against attacks. This should be one of the top priorities of banking sectors in terms of coming up with relevant and effective strategy in handling the challenge of internet banking activities.

REFERENCES

Aboobucker, I., & Bao, Y. (2018). What Obstruct Customer Acceptance of Internet Banking? Security and Privacy, Risk, Trust, and Website Usability and the Role of Moderators. *The Journal of High Technology Management Research, 29(1),* 109-123.

Akgül, Y. (2018). An Analysis of Customers' Acceptance of Internet Banking: An Integration of E-Trust and Service. *E-Manufacturing and E-Service Strategies in Contemporary Organizations,* 154.

Apak, S., Tuncer, G., Atay, E., & Koşan, N. İ. (2012). Insights from Knowledge Management to Radical Innovation: "Internet Banking Applications in the European Union". *Procedia-Social and Behavioral Sciences, 41,* 45-50.

Aribake, F. O. (2015). Impact of ICT Tools for Combating Cybercrime in Nigeria Online Banking: A Conceptual Review. *International Journal of Trade, Economics, and Finance, 6(5),* 272.

Baadel, S., Thabtah, F., & Majeed, A. (2018). Avoiding the Phishing Bait: The Need for Conventional Countermeasures for Mobile Users. *In 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON) (pp. 421-425).* IEEE.

Baykara, M., & Gürel, Z. Z. (2018, March). Detection of Phishing Attacks. *In 2018 6th International Symposium on Digital Forensic and Security (ISDFS) (pp. 1-5).* IEEE.

Bhasin, M. L. (2016). Combatting Bank Frauds by Integration of Technology: Experience of a Developing Country. *British Journal of Research, 3 (3).* 200-212.

Bloodgood, J. M. (2019). Knowledge Acquisition and Firm Competitiveness: The Role of Complements and Knowledge Source. *Journal of Knowledge Management. Vol. 23 No. 1,* pp. 46-66. https://doi.org/10.1108/JKM-09-2017-0430

Bogner WC, & Bansal P. (2007) Knowledge Management as the Basis of Sustained High Performance. *Journal of Management Studies44,*165-188.

Carella, A., Kotsoev, M., & Truta, T. M. (2017). Impact of Security Awareness Training on Phishing Click-Through Rates. In 2017 IEEE International Conference on Big Data (Big Data). pp. 4458-4466. IEEE.

Cassim, F. (2014). Addressing the Specter of Phishing are Adequate Measures in Place to Protect Victims of Phishing. *Comparative and International Law Journal of Southern Africa,* 47(3), 401-428.

Cebi, F., Aydin O. F., & Gozlu, S. (2010) Benefits of Knowledge Management in Banking. *Journal of Transnational Management 15,* 308-321.

Chauhan, V., & Choudhary, V. (2016). E-Banking Services in India: A Broad-Brush Survey of Indian Banks. *IUP Journal of Bank Management, 15(1).*

Chigada, J. (2014). The Role of Knowledge Management in Enhancing Organizational Performance in selected Banks in South Africa, Doctoral Dissertation.

Chin, T., Xiong, K., & Hu, C. (2018). Phish Limiter: A Phishing Detection and Mitigation Approach using Software-Defined Networking. *IEEE Access, 6,* 42516-42531.

Daniels, J., J., & Oberly, J., D. (2019). Employee Education: Training is Key to Curtailing the Risk of a Phishing Attack. https://www.propertycasualty360.com/2019/05/24/how-effective-employee-education-and-training-combats-phishing-attack-risk-414- 155823/?slreturn=20210014080606

Dixit, N. (2016). Acceptance of E-banking among Adult Customers: An Empirical Investigation in India. *Journal of Internet Banking and Commerce,* 15(2).

Eslamkhah, M., & Hosseini Seno, S. A. (2019). Identifying and Ranking Knowledge Management Tools and Techniques Affecting Organizational Information Security Improvement. *Knowledge Management Research & Practice, 17(3),* 276-305.

Frauenstein, E. D. (2013). A Framework to Mitigate Phishing Threats, Doctoral Dissertation, Nelson Mandela Metropolitan University.

Gao, L., & Waechter, K. A. (2017). Examining the Role of Initial Trust in User Adoption of Mobile Payment Services: *An Empirical Investigation. Information Systems Frontiers, 19(3),* 525-548.

Gupta, B., Agrawal, D. P., & Yamaguchi, S. (Eds.). (2016). Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security. *IGI Global.*

Hislop, D., Murray, P. A., Shrestha, A., Syed, J., & Mouzughi, Y. (2018). Knowledge Management: Potential Future Research Directions. *In the Palgrave Handbook of Knowledge Management,* pp. 691-703. Palgrave Macmillan, Cham.

Hong, J. (2012). The State of Phishing Attacks. *Communications of the ACM, 55(1),* 74-81.

Jain, A. K., & Gupta, B. B. (2017). Phishing Detection: Analysis of Visual Similarity-based Approaches. *Security and Communication Networks.*

Jain, A. K., & Gupta, B. B. (2016). Comparative Analysis of Features based Machine Learning Approaches for Phishing Detection. *In 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom),* pp. 2125-2130. IEEE.

Jang-Jaccard, J., & Nepal, S. (2014). A Survey of Emerging Threats in Cybersecurity. *Journal of Computer and System Sciences, 80(5),* 973-993.

Jennex, M. E., & Durcikova, A. (2019). Integrating IS Security with Knowledge Management: What can Knowledge Management Learn from IS Security Vice Versa? *In Effective Knowledge Management Systems in Modern Society,* pp. 267-283. IGI Global.

Jensen, M., Durcikova, A., & Wright, R. (2017, January). Combating Phishing Attacks: A Knowledge Management Approach. *In Proceedings of the 50th Hawaii International Conference on System Sciences.*

Kaabachi, S., Ben Mrad, S., & Petrescu, M. (2017). Consumer Initial Trust toward Internet-only Banks in France. *International Journal of Bank Marketing, 35(6),* 903-924.

Kamwibua, D. K. (2017). Why there is Low Adoption of Internet Banking by Consumers in Kenya. Doctoral Dissertation, United States International University-Africa.

Khedmatgozar, H. R., & Shahnazi, A. (2018). The Role of Dimensions of Perceived Risk in the Adoption of Corporate Internet Banking by Customers in Iran. *Electronic Commerce Research, 18(2),* 389-412.

Lee, O. K. D., Choi, B., & Lee, H. (2020). How do Knowledge Management Resources and Capabilities Pay-Off in Short term and Long Term? *Information & Management, 57(2),* 103166.

Lord, N. (2020). Social Engineering Attacks: Common Techniques & How to Prevent an Attack. https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack

Mann, I. (2017). Hacking the Human: Social Engineering Techniques and Security Countermeasures. Routledge.

Meihami, B., & Meihami, H. (2014). Knowledge Management a Way to Gain a Competitive Advantage in Firms (Evidence of Manufacturing Companies). *International Letters of Social and Humanisti.c*

Memon, S. B., Rizvi, W. H., & Syed, S. (2017). Operationalization of Knowledge Management in Knowledge-Intensive Pakistani Banks: A Qualitative Case Studies. *Knowledge and Performance Management, 1(1),* 36-45.

Merlyn, P. R., & Välikangas, L. (1998). From Information Technology to Knowledge Technology: Taking the User into Consideration. *Journal of Knowledge Management, 2(2),* 28-35.

Mills, A. M., & Smith, T. A. (2011). Knowledge Management and Organizational Performance: A Decomposed View. *Journal of Knowledge Management, Vol. 15 No. 1,* pp. 156-171. https://doi.org/10.1108/13673271111108756.

Nero, P. J., Wardman, B., Copes, H., & Warner, G. (2011, November). Phishing: Crime that Pays. *In 2011 E-Crime Researchers Summit (pp. 1-10).* IEEE.

Nonaka, I., & Takeuchi, H. (1995). The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation? *Oxford University Press*.

Olodude, O. O., & Oladejo, B. F. (2013). Enhanced Customer-based Knowledge Management System for Product Generation in the Banking System. *Annals. Computer Science Series, 11(1),* 129-137.

Omotayo, F. O. (2015). Knowledge Management as an Important Tool in Organizational Management: A Review of Literature Library. *Library Philosophy and Practice* 1, *no. 2015 (2015)*, 1-23.

Palmer, D. (2020). What is Phishing? Everything you need to Know to Protect yourself from Scam Emails and More. *https://www.zdnet.com/article/what-is-phishing-how-to-protect-yourself-from-scam-emails-and-more/*

Perry, P. (2020). Knowledge is Power — How to Prevent Phishing Attacks. https://www.perryprotech.com/blog/knowledge-is power- how-to-prevent-phishing-attacks/

Pymnts, (2017). Phishing Attacks Hit New Record in 2016. https://www.pymnts.com/fraud attack/2017/phishing-attacks-hit-new-record-in-2016/

Ragsdell, G. (2009). Managing Knowledge about Knowledge Management: 'Practising What We Teach'. *Innovation in Teaching and Learning in Information and Computer Sciences, 8(1),* 21-26.

Rashed, M. (2016). The Readiness of Banks in Knowledge Management: A Study of Three Private Commercial Banks in Bangladesh. *Journal of Business Finance. 5(2),* 12-19.

Robb, D. (2020). Why Enterprises Struggle to Thwart Phishing Attacks? https://www.cioinsight.com/security/why-enterprises-struggle to-thwart-phishing-attacks.html

Siriwardena, N., & Gillam**, S.** (2014). Individual Practice and How to Improve it. https://pubmed.ncbi.nlm.nih.gov/24865340/

Stafford, C. D. (2020). Weakest Link: Assessing Factors that Influence Susceptibility to Falling Victim to Phishing Attacks and Methods to Mitigate. Doctoral Dissertation, Utica College.

Sukumaran, S., Amalathas, S. S., Simon, C. G. K., Mustapha, S. S., Hashem, I. A. T., & Zulkifli, A. F. (2018, October). A Case Study on Knowledge Management Implementation in the Banking Sector–Issues and Challenges. In *2018 Fourth International Conference on Advances in Computing, Communication & Automation (ICACCA),* pp. 1-6. IEEE.

Thakur, H., & Kaur, S. (2016). A Survey Paper on Phishing Detection. *International Journal of Advanced Research in Computer Science, 7(4).*

Uğurlu, Ö. Y., & Kızıldağ, D. (2013). A Comparative Analysis of Knowledge Management in the Banking Sector: An Empirical Research. *European Journal of Business and Management 5, No. 16*, 12-19.

Usman, A. K. (2018). An Investigation into the Critical Success Factors for E-Banking Frauds Prevention in Nigeria, Doctoral Dissertation, University of Central Lancashire.

Viswanadham, N. (2017). Is the Banking Organization Providing IT Enabled Services with Accuracy and Measured Against the Agreed Specifications? *International Finance and Banking, 4(1),* 44.